REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

Claims 19 and 20 are cancelled without prejudice. Claim 1 refers to operating modes to more clearly distinguish between "modes" and "domains" and 1 incorporates the previous wording of claim 2: "at least one of the devices being operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain." Claim 10 is similarly amended incorporating the features of claim 11.

The claimed secure and non-secure domains provide a mechanism for handling security at the hardware level. The non-secure and secure domains effectively establish separate worlds: a non-secure world including all hardware and software accessible to non-secure applications that do not require security, and a secure world including all hardware and software that is only accessible when executing secure mode. The non-secure and secure domains/worlds are different from modes of operation. Typically, operation modes are only applicable to certain types of devices such as processors, e.g., a processor that can operate in either user mode or privileged mode. Operating modes within certain devices like processors exist in both the non-secure domain and the secure domain. But not all devices that can be connected to the device bus (see Figure 1) employ modes of operation. This is the reason why the independent claims were amended to state that "at least one of the devices" is operable in a plurality of modes.

Claims 1 and 10 have been amended to clarify further the purpose of the domain signal "to determine whether the access defined by the memory access request is allowed to proceed." Thus, the domain signal issued in association with any memory access request restricts access to secure data.

The new text for claims 2 and 11 further emphasizes the distinction between modes and domains in one non-limiting example embodiment: "for said at least one of the devices, said plurality of modes are replicated in said secure domain and said non-secure domain."

The Examiner makes a provisional double patenting rejection of certain claims in view of claims in co-pending application 10/714,481. This provisional rejection is respectfully traversed.

Contrary to the position taken by the Examiner on page 9, the "flags" associated with each entry in the memory unit described in co-pending application 10/714,481 are an entirely different entity from the "domain signal," claimed in the instant application, which is issued with each memory access request. The flags described in co-pending application 10/714,481 are held in association with the memory unit, and for each entry of the memory unit, identify whether that entry contains secure data or non-secure data. In contrast, the claimed domain signal is issued by a device when issuing a memory access request to identify whether the memory access request pertains to the secure domain or the non-secure domain. Withdrawal of the double patenting rejection is requested.

The Examiner rejects all claims 1-20 under 35 U.S.C. §102(e) for anticipation based upon US-A-2003/0101322 (Gardner). This rejection is traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Gardner fails to satisfy this rigorous standard.

Gardner describes a mechanism for protecting user application data so that it can be kept

secret from root and other users (see Figure 6 and the associated description in paragraphs 0189 to 0193). There are four privilege levels PLO to PL3: PL0 is the most privileged level of the processor, and PL3 is the least privileged level of the processor (see paragraphs 0018 and 0019). The operating system runs at a privilege level PL2, and user applications run at the lower privilege level PL3 (see paragraph 0019). Figure 6 illustrates an approach where a user application operating at the lowest privilege level keeps its data secure from other users. Gardner refers to such user applications that require their data to be kept secure as "secure user applications." To accomplish that security, Gardner uses protection keys which allow a secure user application "to access a page of memory in memory 74 that nobody else can access, including root or anything running at PL2 or above" (see paragraph 0190). Code executing at the protection level PLO inserts the protection keys into protection key registers (paragraph 0191).

Gardner's approach is very different than that recited in claims 1 and 10. In contrast to Gardner's use of protection keys to secure certain data of a user application, security of data in the instant claims is managed at the hardware level on a domain basis. Data handled by the secure domain is not accessible from the non-secure domain. A domain signal issued with each memory access request is used to enforce this security. The domain signal is used to determine whether the access defined by any particular memory access request is allowed to proceed. In particular, if the domain signal identified that the memory access request pertained to a non-secure domain, then that access request would not be allowed to proceed if the memory access request was seeking to access secure data. Gardner does not control access to data based on domains and associated domain signals included with memory access requests. Instead, Gardner uses protection keys managed by the highest privileged level PLO to keep the data of particular "secure" user applications secret, and hence not accessible by other applications.

Regarding the statement of rejection based on Gardner, the office action equates certain features in Gardner with certain features in the claims in a way that is somewhat confusing and at times inconsistent. For example, the office action equates the plurality of operation modes with *both* the execution privilege levels in Gardner and the term "user processes" in paragraph 0189. But, on that basis, it is not clear what feature of Gardner the Examiner equates with the secure and non-secure domains. As is clear from claim 1, the secure domain and non-secure domain represent the mechanism by which data is kept secure.

Gardner's paragraphs 0189 and 0026 appear to be the main paragraphs being used in the office action in rejecting claims 1 and 10. As explained above, paragraph 0189 is associated with Figure 6 and describes secure and non-secure *user applications/processes*—not secure and non-secure *domains*. Paragraph 0026 refers to a "domain" and mentions that secure platform 40 ensures that one domain cannot accidentally or intentionally access another domain's memory. It is not clear from paragraph 0026 what the domains being referred to are, but paragraphs 0031 and 0032 describe that the operating system image can be partitioned into independent protection domains which operate at the PL2 privilege level. The multiple protection domains are protected from each other through the memory protection capabilities of the four privilege level processor hardware 32 (paragraph 0032).

Hence, the protection domains in Gardner are not the mechanism used to keep data secure, and hence, are different from the claimed secure domain and non-secure domains. There is no disclosure in Gardner of a *memory access request* pertaining to either a secure domain or a non-secure domain, as recited in claims 1 and 10.

Nor is there any teaching of a *memory access request including a domain signal identifying whether the memory access request pertains to the secure domain or non-secure*

domain. The office action suggests that the feature of the domain signal is disclosed by paragraph 0189. But paragraph 0189 makes no reference to domains at all, and merely describes that secure user applications (i.e., applications that want their data to be kept secure from other users) are distinguishable from non-secure user applications through appropriate setting of a "magic number" or ELF header. Although this information enables different types of applications to be distinguished from one another, it has nothing to do with issuing memory access requests or managing access to data associated with those memory access requests. Claims 1 and 10 recite that the domain signal is included with each memory access request. The domain signal is used "to determine whether the access defined by the memory access request is allowed to proceed" (quoted from claim 10). No such domain signal or use of that domain signal to determine whether to allow an access request to proceed is disclosed in Gardner.

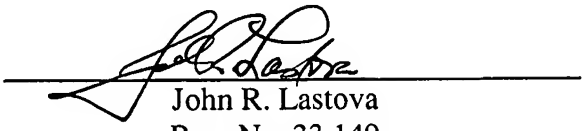
Claims 1 and 10 also recite that the data processing apparatus has a plurality of devices coupled to the device bus. In contrast, Gardner shows only a single processor coupled to a memory in Figure 3. Hence, Gardner does not disclose "a plurality of devices coupled to a device bus, each operable to issue a memory access request ...."

Because Gardner lacks multiple features recited in the independent claims 1 and 10 and fails to address the particular problem solved by those claims, rejection based on Gardner is improper and should be withdrawn.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL:sd
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100